UNITED STATES OF AMERICA	)	
	)	**RULING: Defense Motions**
v.	)	**For Findings of Not Guilty -**
	)	**RCM 917**
Manning, Bradley E.	)	
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	
Joint Base Myer-Henderson Hall	)	**18 July 2013**
Fort Myer, Virginia 22211	)	

On 4 July 2013, the Defense filed four Motions for Findings of Not Guilty in accordance with (IAW) RCM 917 for the following offenses alleging that the Government has failed to present evidence to prove one or more elements of those offenses (AEs 593-596).

(1) Aiding the Enemy, in violation of Article 104, UCMJ (the specification of Charge I). The Defense challenges one element and specifically asserts the Government has not provided evidence that proves the accused knowingly gave intelligence information to certain persons, namely: al Qaeda, and al Qaeda in the Arabian Peninsula. The Court's instructions define "knowingly." "'Knowingly' requires actual knowledge by the accused that by giving the intelligence to the 3rd party or intermediary or in some other indirect way, that he was actually giving intelligence to the enemy through this indirect means. This offense requires that the accused had a general evil intent in that the accused had to know he was dealing, directly or indirectly, with an enemy of the United States. 'Knowingly' means to act voluntarily and deliberately. A person cannot violate Article 104 by committing an act inadvertently, accidentally, or negligently that has the effect of aiding the enemy."

(2) Fraud and Related Activity with Computers, in violation of 18 U.S.C. §1030(a)(1) and Article 134, UCMJ (specification 13 of Charge II). The Defense asserts the Government has not provided evidence that the accused exceeded authorized access on a Secret Internet Protocol Router Network (SIPR) computer;

(3) Stealing, Purloining, or Knowingly Converting Records Belonging to the United States, in violation of 18 U.S.C. §641 and Article 134, UCMJ (specifications 4, 6, 8, 12, and 16 of Charge II);

(4) Particularized motion with respect to specification 16 of Charge II.

On 11 July 2013, the Government filed three briefs in opposition (AEs 599-601). On 12 July 2013, the Defense filed a reply brief to the Government's brief in response to the Defense Motion for a Finding of Not Guilty on the 18 U.S.C. §641 offenses (AE 603). On 16 July 2013, the Defense supplemented their brief on the 18 U.S.C. §641 offenses with an email filing (AE 608). On 17 July 2013, the Government filed a supplemental response in opposition to the email filing (AE 606). On 15 July 2013, the Court heard oral argument on the RCM 917 Motions for the specification of Charge I (Aiding the Enemy, in violation of Article 104, UCMJ) and specification 13 of Charge II (Fraud and Related Activities with Computers, in violation of

APPELLATE EXHIBIT 609
PAGE REFERENCED:
PAGE ___ OF ___ PAGES

18 U.S.C. §1030(a)(1) and Article 134, UCMJ). On 18 July 2013, the parties will present oral argument regarding the RCM 917 Motions for specifications 4, 6, 8, 12, and 16 of Charge II (Stealing, Purloining, or Knowingly Converting Records Belonging to the United States, in violation of 18 U.S.C. §641 and Article 134, UCMJ).

This ruling sets forth the legal standard used by the Court in determining motions for a finding of not guilty under RCM 917 and findings of fact and conclusions of law regarding the RCM 917 motions for Article 104, Aiding the Enemy and 18 U.S.C. §1030(a)(1)/Article 134. After hearing oral argument on the motions, the Court will issue a supplemental ruling for the 18 U.S. C. §641/Article 134 offenses.

The Law:

1. PFC Manning has elected trial by military judge alone, thus, the Court acts in two capacities. As the fact finder, the court must determine whether the Government has proven each and every element of each offense charged beyond a reasonable doubt. In considering this Motion for a finding of Not Guilty by the Defense, the Court acts in its interlocutory capacity and decides the motion under the lesser standard required in RCM 917.

2. RCM 917 Standard: A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged. The evidence shall be viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses. RCM 917(d).

3. Should the Court grant a finding of not guilty to an element of the greater offense for an offense to which PFC Manning has pled guilty to a lesser included offense, the Government would be precluded from proceeding on the greater offense. RCM 917(e).

RCM 917 – Article 104, UCMJ, Aiding the Enemy:

Findings of Fact:

1. The Court has examined the prosecution exhibits, defense exhibit J, and testimony of the witnesses set forth in the Witnesses/Evidence portion of the Government brief (AE 600). This provides some evidence that between on or about 1 November 2009 and 27 May 2010 the accused:

(1) was an enlisted Soldier who was a trained all-source intelligence analyst (35F). The accused trained and passed 35F Advanced Individual Training (AIT). This training identified al Qaeda as a terrorist group. It also included a lesson on terrorist use of the internet and lessons on information security (INFOSEC) to include the classification process, why information is classified, restrictions on access to classified information, storage and safekeeping of classified information to include individual responsibility to safeguard classified information and to ensure that unauthorized persons do not gain access to classified information. The training further instructed 35F Soldiers that the enemy will attempt to discover how and when the U.S. is

conducting operations. As such, critical information (anything that helps the enemy obtain an advantage over the U.S.) including tactics, techniques and procedures (TTPs), unit capabilities and intent, and personal/family information must be protected. The training completed by the accused warned that operational activities should not be discussed on the internet or on email, and Soldiers should always assume the adversary is reading posted material.

(2) prepared a slide show dated 13 Jun 08 entitled "Operations Security (OPSEC)" that defined critical information, identified adversaries, listed common OPSEC leaks, and concluded with the need to avoid public disclosure of critical information to include posting information on the internet.

(3) signed two non-disclosure agreements dated 7 April 2008 and 17 September 2008, respectively, where he acknowledged that he received and understood a security indoctrination concerning the nature and protection of classified information including the procedures to be followed in ascertaining whether persons to whom the accused contemplates disclosing classified information have been approved for access to it and that the accused has been advised that the unauthorized disclosure of classified information could cause damage or irreparable injury to the U.S. or could be used to the advantage of a foreign nation.

(4) maintained a variety of intelligence publications on his external hard drive. Portions of the publications address use of the internet by terrorist organizations and opposing forces.

(5) deployed to Forward Operating Base (FOB) Hammer, Iraq on or about October 2009 and remained deployed there past May 2010. He had access to the classified information on the Secret Internet Protocol Router (SIPR) network on the Defense Common Ground System-Army (DCGS-A) computers in the 2nd Brigade (BDE) SCIF. The accused was working as an all-source intelligence analyst, using the sigacts on the CIDNE-I database to develop intelligence products that involved pattern analysis. The accused downloaded, indexed, and plotted CIDNE-I sigacts on maps based on locations and enemy threats. The accused was aware that the enemy also engaged in similar pattern analysis about U.S. TTPs and movements. The accused sent to WikiLeaks the same CIDNE-I database and sigacts he used to develop pattern analysis with the intent that it be disclosed to the public.

(6) accessed the ACIC report published on 18 March 2008 entitled "Wkileaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" on 1 December 2009, 29 December 2009, 1 March 2010 and 7 March 2010. The ACIC report was a counterintelligence analysis report analyzing the threat posed by Wikileaks.org following the release of 2000 pages of U.S. Army Tables of Equipment in Iraq and Afghanistan from April 2007 and release of other classified U.S. information. The report listed as an intelligence gap "Will the Wikileaks.org Web site be used by FISS, foreign military services, foreign insurgents, or terrorist groups to collect sensitive or classified U.S. Army information posted to the Wikileaks.org Web site?". The report also listed a conclusion that "It must be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the Wikileaks.org Web site. Web sites similar to Wikileaks.org will continue to proliferate and will continue to represent a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army for the foreseeable future." The accused sent the ACIC report

to Wikileaks between on or about 15 February 2010 and 15 March 2010 with the intent that it be disclosed to the public.

(7) on 14 February 2010 searched for IRR 5 391 0014 08 dated 23 March 2008 entitled "Internet Web Postings of Classified and for Official Use Only Documents". The IRR discussed Wikileaks as a publicly accessible Internet website where leaked information, including classified information, can be published to the public anonymously. The report described the threat to the Marine Corps of publication of Marine Corps sensitive or classified information. On 15 February 2010, the accused moved the IRR to his personal computer.

(8) on 14 February 2010, searched for a report dated 7 January 2010 entitled "MARFOREUR TRIP REPORT (MTR) discussing Marine Corps monitoring of Chaos Communication Congress 26C3 Here Be Dragons Conference held 26-30 December 2009." The report discussed the conference discussion on Wikileaks as a publicly accessible Internet website where leaked information, including classified information, can be published to the public anonymously. On 15 February 2010, the accused moved the MTR to his personal computer.

(9) made statements in his 5 – 18 March 2010 chats with Press Association/Julian Assange indicating his understanding that WikiLeaks was "like an intelligence agency minus the anonymous sources" and that WikiLeaks was seeking to publish Government controlled information sent to them by the accused and other donors.

(10) made statements in his May 2010 chats with Adrian Lamo admitting that he gave WikiLeaks the following classified information from the SIPRNET: a database of half a million events during the Iraq war…from 2004-2009…with reports, date time groups, lat-lon locations, casualty figures, 260,000 state department cables from embassies and consulates all over the world, classified cable from U.S. embassy Reykyavik on Icesave dated 13 Jan 10, the Gharani airstrike video from CENTCOM.smil.mil; the Apache video, and the JTF-GTMO papers. The accused also made statements that the 260,000 classified cables from the Net-Centric Diplomacy database that he sent to WikiLeaks would be released to the public in searchable format.

Conclusion of Law:

The accused's training and experience as an all source intelligence analyst, his preparation of intelligence products while deployed in Iraq, a combat zone, using the CIDNE-I database while contemporaneously sending the entire database to WikiLeaks for public disclosure and world-wide publication, the volume of classified information from the Department of Defense and the Department of State that the accused admitted to disclosing to WikiLeaks, and the accused's search for and downloading of counterintelligence documents reporting the threat posed by WikiLeaks, considered together, provide some evidence from which, together with all reasonable inferences and applicable assumptions, viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses, could reasonably tend to establish that the accused actually knew he was dealing with the enemy and actually knew that by sending such information to WikiLeaks with the intent that it be broadcast to the public, he was knowingly providing intelligence to the enemy. The "intelligence gap" evidence in the ACIC report as well

as laudable motive evidence by the accused goes to the weight of the evidence, a decision properly determined by the fact-finder.

RCM 917 – 18 U.S.C. §1030(a)(1), Fraud and Related Activity with Computers

Findings of Fact:

1. The Government's theory for specification 13 of Charge II is that the accused "exceeded authorized access" by accessing and downloading classified information using Wget, unauthorized software on Army computers and on the DCGS-A computers.

2. 18 U.S.C. §1030(e)(6) defines the phrase "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." There is a split in the federal circuits regarding whether this definition is an access only restriction or whether a restriction on use of the information accessed can violate the statute as well. *See generally Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, but Illegal in Miami, Dallas, Chicago, and Boston,* 87-JAN Fla. B.J. 36 (January 2013).

3. This Court has issued two previous rulings dated 8 June 2012 (AE 139) and 18 July 2012 (AE 218) in response to Defense Motions to Dismiss specifications 13 and 14 of Charge II. In those rulings, the Court found ambiguity in the statute, applied the rule of lenity, and ruled that the Court would instruct in accordance with the narrow interpretation that "exceeds authorized access" is limited to violations of restrictions on access to information and not restrictions on the use of information. The Court specifically ruled "Restrictions on access to classified information are not limited to code based or technical restrictions on access. Restrictions on access to classified information can come from a variety of sources, to include regulations, user agreements, and command policies. Restrictions on access can include manner of access. User agreements can also contain restrictions on access as well as restrictions on use. The two are not mutually exclusive. The Court does not find this issue capable of resolution prior to the presentation of evidence. These issues are properly decided after the formal presentation of the evidence as a motion for a finding of not guilty or a motion for finding that the evidence is not legally sufficient."

4. The accused pled guilty to lesser included offenses of specifications 13 and 14 of Charge II. The Government advised the Court it is not going forward with the greater offense for specification 14 of Charge II.

5. In line with the Court's 18 July 2012 order, the Defense challenges the Government theory on legal grounds and moves for a Finding of Not Guilty. Specifically, the Defense argues that there were no restrictions on the accused's access to the Department of State (DOS) Net-Centric Diplomacy (NCD) database or his ability to download the records in the NCD imposed by either DOS or DoD. The accused would have the same access to the NCD whether he used Wget to download the files rapidly or whether he downloaded them slowly by click/save. Thus, the Defense argues, even if Wget is an unauthorized program, it is not an access restriction for purposes of 18 U.S.C. §1030(a)(1).

6. The Defense cites *Wentworth-Douglass Hospital v. Young & Novis Professional Association,* 2012 WL 2522963 (D.N.H.), a civil case under 18 U.S.C. 1030(a)(2)(C) where the defendants violated a hospital computer use policy by connecting large removable storage devices to download information. The court held that this was a use restriction not an access restriction ("Of course, the distinction between an employer-imposed "use restriction" and an "access restriction" may sometimes be difficult to discern, since both emanate from policy decisions made by the employer – decisions about who should have what degree of access to the employer's computer and stored data and, once given such access, the varying uses to which each employee may legitimately put those computers and the data stored on them. But, simply denominating limitations as "access restrictions" does not convert what is otherwise a use policy to an access restriction. Here, the hospital's policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an 'access' restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access. An employee who is given access to hospital data need not "hack" the hospital's computers or circumvent technological access barriers in order to impermissibly copy that data onto an external storage device. The offending conduct in this case is misuse of data the employee was authorized to access, not an unauthorized access of protected computers and data.")

7. The Government has presented testimony by Special Agent (SA) David Shaver, Mr. Jason Milliman, CPT Thomas Cherepko, and Mr. Mark Kirtz that Wget is not authorized software for a DCGS-A computer and, even if it was, Wget, as executable software, was required to be installed by Mr. Milliman on the DCGS-A computers. The Government has also presented evidence that the accused downloaded Wget to his user profile on the DCGS-A computer he used in the SCIF.

8. The Defense has elicited testimony from Mr. Weaver and COL Miller that Wget was no different than executable software such as games, and, even if technically prohibited, these prohibitions were not enforced by the chain of command.

Conclusions of Law:

1. The Court adheres to its rulings on interpreting "exceeding authorized access" in AE 139 and 218.

2. Unlike *Wentworth-Douglass Hospital*, this case involves classified information belonging to the U.S. government. The accused is charged under 18 U.S.C. §1030(a)(1). Although the definition for "exceeds authorized access" is the same for all of the sections of 18 U.S.C. 1030, access restrictions on classified information can be more stringent than for other information and can include manner of access restrictions designed to ensure the security and protection of the classified information and to prevent the classified information from exposure to viruses, trojan horses or other malware.

3. Evidence that the accused used unauthorized software, Wget, to access and download the classified records charged in specification 13 of Charge II provides some evidence from which,

together with all reasonable inferences and applicable assumptions, viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses, could reasonably tend to establish that the accused "exceeded authorized access" on a SIPR computer. The countervailing evidence presented by the Defense goes to the weight of the evidence, a decision properly determined by the fact-finder.

Ruling: The Defense Motions for a Finding of Not Guilty for the specification of Charge 1 and specification 13 of Charge II are **Denied.** The Court will issue a supplemental ruling regarding the Defense Motions for a Finding of Not Guilty for Specifications 4, 6, 8, 12, and 16 of Charge II in due course.

So **Ordered** this 18th day of July 2013.

DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit